

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-140450

(43)Date of publication of application : 17.05.2002

(51)Int.Cl. G06F 17/60
 G10K 15/02
 G10L 19/00
 H04M 1/00
 H04M 11/00
 // G06F 13/00

(21)Application number : 2000-334201

(71)Applicant : SANYO ELECTRIC CO LTD

(22)Date of filing : 01.11.2000

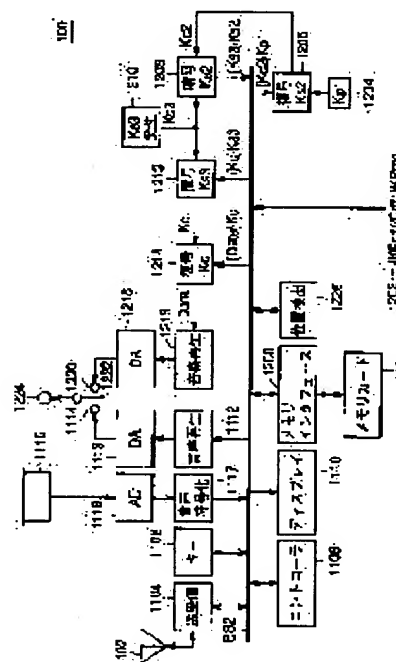
(72)Inventor : MATSUURA TAKENORI

(54) DATA DISTRIBUTING SYSTEM AND DATA TERMINAL EQUIPMENT

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a data distributing system and data terminal equipment capable of receiving enciphered contents data related with positional information.

SOLUTION: A portable telephone set 100 is provided with a position detecting part 1226. The position detecting part 1226 detects the present position of the portable telephone set 100 by a GPS. A controller 1106 transmits the present position of the portable telephone set 100 detected by the position detecting part 1226 through a transmitting/receiving part 1104 to a distributing server at the time requesting the distribution of the enciphered contents data. Then, the controller 1106 receives the enciphered contents data related with the present position through the transmitting/receiving part 1104, and records and/or reproduces the enciphered contents data to/from a memory card 110.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

What is claimed is:

1. A data terminal device for receiving an enciphered content data that is content data enciphered, and a license for reproducing the enciphered content data from a distributing server, and for recording and/or reproducing the enciphered content data and the license to/from a data recording device, the data terminal device comprising:

a transmitting/receiving part for performing a communication with the external;

an interface for controlling data transfer with the data recording device;

a key operating part for inputting a direction; and

a control part,

wherein the control part receives an enciphered content data related with a present position and a license for reproducing the enciphered content data from the distributing server via the transmitting/receiving part, in response to a request for receiving the enciphered content data input through the key operating part, and records the received enciphered content data and the license in the data recording device via the interface.

2. The data terminal device of claim 1, wherein the control part transmits the present position as position information as well as a distribution request of the enciphered content data to the distributing server via the transmitting/receiving part.

3. The data terminal device of claim 2, further comprising a position detecting part for detecting the present position, wherein the control part transmits the detected present position to the distributing server via the transmitting/receiving part.

4. The data terminal device of claim 3, wherein the position detecting part detects the present position by a global positioning system.

【特許請求の範囲】

【請求項1】 コンテンツデータを暗号化した暗号化コンテンツデータと、前記暗号化コンテンツデータを再生するためのライセンスとを配信サーバから受信し、前記暗号化コンテンツデータおよび前記ライセンスをデータ記録装置に記録および／または再生するデータ端末装置であって、

外部との通信を行なう送受信部と、

前記データ記録装置とのデータ授受を制御するインタフェースと、

指示を入力するためのキー操作部と、

制御部とを備え、

前記制御部は、前記キー操作部を介して入力された暗号化コンテンツデータの受信要求に応じて、現在位置に関連する暗号化コンテンツデータと前記暗号化コンテンツデータを再生するライセンスとを前記送受信部を介して前記配信サーバから受信し、その受信した暗号化コンテンツデータとライセンスとを前記インタフェースを介して前記データ記録装置に記録する、データ端末装置。

【請求項2】 前記制御部は、前記暗号化コンテンツデータの配信要求とともに前記現在位置を位置情報として前記送受信部を介して前記配信サーバへ送信する、請求項1に記載のデータ端末装置。

【請求項3】 前記現在位置を検出する位置検出部をさらに備え、

前記制御部は、前記検出した現在位置を前記送受信部を介して前記配信サーバへ送信する、請求項2に記載のデータ端末装置。

【請求項4】 前記位置検出部は、グローバルポジショニングシステムによって前記現在位置を検出する、請求項3に記載のデータ端末装置。

【請求項5】 前記制御部は、コンサート会場の位置を前記現在位置として前記送受信部を介して前記配信サーバへ送信し、前記コンサート会場で演奏されている曲と同じ暗号化音楽データを前記送受信部を介して受信する、請求項1から請求項4のいずれか1項に記載のデータ端末装置。

【請求項6】 前記制御部は、前記暗号化音楽データを再生するライセンスを通常料金よりも安い料金で受信する、請求項5に記載のデータ端末装置。

【請求項7】 表示部をさらに備え、

前記制御部は、前記現在位置に関連する画像データを前記送受信部を介して受信し、その受信した画像データを前記表示部に表示する、請求項5または請求項6に記載のデータ端末装置。

【請求項8】 前記暗号化コンテンツデータは暗号化音楽データであり、

前記暗号化音楽データを再生した音楽データを外部装置へ出力するための端子をさらに含み、

前記制御部は、前記配信サーバにおいて再生された音楽

データを受信し、その受信した音楽データを前記端子へ与え、前記音楽データの受信要求が前記キー操作部から入力されると前記配信サーバへ暗号化音楽データの配信要求を送信する、請求項1に記載のデータ端末装置。

【請求項9】 コンテンツデータを暗号化した暗号化コンテンツデータと、前記暗号化コンテンツデータを再生するライセンスとを保持する配信サーバと、

前記配信サーバから前記暗号化コンテンツデータおよび前記ライセンスを受信し、その受信した暗号化コンテンツデータおよびライセンスをデータ記録装置に記録および／または再生するデータ端末装置とを備え、

前記配信サーバは、前記暗号化コンテンツデータの配信要求を送信した前記データ端末装置の現在位置に関連した暗号化コンテンツデータを前記データ端末装置へ配信する、データ配信システム。

【請求項10】 前記配信サーバは、前記現在位置に関連した暗号化コンテンツデータの配信要求を受信すると、電話網によって位置情報を取得する位置情報センタ一から前記現在位置を受信する、請求項9に記載のデータ配信システム。

【請求項11】 前記配信サーバは、前記データ端末装置から前記現在位置を取得する、請求項9に記載のデータ配信システム。

【請求項12】 前記配信サーバは、携帯電話網を構成する基地局から前記現在位置を取得する、請求項9に記載のデータ配信システム。

【請求項13】 前記配信サーバは、前記現在位置を受信してからその現在位置に関連する暗号化コンテンツデータを検索し、その検索した暗号化コンテンツデータを前記データ端末装置へ配信する、請求項9から請求項12のいずれか1項に記載のデータ配信システム。

【請求項14】 前記配信サーバは、予め位置情報によって分類された暗号化コンテンツデータを保持し、前記現在位置を受信するとその現在位置に関連する暗号化コンテンツデータを前記データ端末装置へ配信する、請求項9から請求項12のいずれか1項に記載のデータ配信システム。

【請求項15】 前記配信サーバは、コンサート会場の位置を前記現在位置として前記データ端末装置から受信し、前記コンサート会場で演奏されている曲と同じ暗号化音楽データを前記データ端末装置へ配信する、請求項9から請求項14のいずれか1項に記載のデータ配信システム。

【請求項16】 前記配信サーバは、前記暗号化音楽データを再生するライセンスを通常料金よりも安い料金で前記データ端末装置へ配信する、請求項15に記載のデータ配信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、コピーされた情

報に対する著作権保護を可能とするデータ配信システムおよびデータ端末装置に関するものである。

【0002】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】したがって、このような情報通信網上において音楽データや画像データ等の著作権者の権利が存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【0007】しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【0008】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0009】この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【0010】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書とを暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【0011】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

【0012】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話に装着する。携帯電話は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【0013】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【0014】

【発明が解決しようとする課題】しかし、暗号化コンテンツデータの配信をサーバへ要求する場合、ユーザとしては、現在位置に関連する暗号化コンテンツデータの配信を要求したい場合がある。特に、旅行などで各地域を訪れた場合、その地域に関連する音楽を聴きたいときがあり、その場合、その地域に関連する音楽を迅速に受信できれば便利である。

【0015】それゆえに、この発明の目的は、位置情報に関連する暗号化コンテンツデータを受信可能なデータ配信システムおよびデータ端末装置を提供することである。

【0016】

【課題を解決するための手段および発明の効果】この発明によるデータ端末装置は、コンテンツデータを暗号化した暗号化コンテンツデータと、暗号化コンテンツデータを再生するためのライセンスとを配信サーバから受信し、暗号化コンテンツデータおよびライセンスをデータ記録装置に記録および／または再生するデータ端末装置

コンテンツ
データ
暗号化

であって、外部との通信を行なう送受信部と、データ記録装置とのデータ授受を制御するインタフェースと、指示を入力するためのキー操作部と、制御部とを備え、制御部は、キー操作部を介して入力された暗号化コンテンツデータの受信要求に応じて、現在位置に関連する暗号化コンテンツデータと暗号化コンテンツデータを再生するライセンスとを送受信部を介して配信サーバから受信し、その受信した暗号化コンテンツデータとライセンスとをインタフェースを介してデータ記録装置に記録する。

【0017】この発明によるデータ端末装置は、データ端末装置の現在位置に関連する暗号化コンテンツデータと、その暗号化コンテンツデータを再生するライセンスとを受信し、データ記録装置に記録および／または再生を行なう。

【0018】したがって、この発明によれば、移動中などに各地域に関連する音楽を楽しむことができる。

【0019】好ましくは、データ端末装置の制御部は、暗号化コンテンツデータの配信要求とともに現在位置を位置情報として送受信部を介して配信サーバへ送信する。

【0020】データ端末装置においては、制御部は、暗号化コンテンツデータの配信要求を配信サーバへ送信するとともに、データ端末装置の現在位置を配信サーバへ送信する。つまり、データ端末装置は、位置情報の発信機能を有する。そうすると、配信サーバは、受信した現在位置に関連する暗号化コンテンツデータを抽出し、データ端末装置へ配信する。

【0021】したがって、この発明によれば、正確な現在位置を配信サーバへ送信することができる。

【0022】好ましくは、データ端末装置は、現在位置を検出する位置検出部をさらに備え、制御部は、検出した現在位置を送受信部を介して配信サーバへ送信する。

【0023】位置検出部は、データ端末装置の現在位置を検出し、制御部は位置検出部が検出した現在位置を受取り、送受信部を介して配信サーバへ送信する。つまり、データ端末装置は、位置情報の検出および発信機能を有する。

【0024】したがって、この発明によれば、データ端末装置は自ら位置検出と、その検出した位置情報を配信サーバへ送信することができる。

【0025】好ましくは、データ端末装置の位置検出部は、グローバルポジショニングシステムによって現在位置を検出する。

【0026】位置検出部は、少なくとも3個または4個の衛星から送られてくる信号に基づいてデータ端末装置の現在位置を検出する。そして、制御部は位置検出部がグローバルポジショニングシステム (GPS (Global Positioning System)) によって検出した現在位置を受取り、配信サーバへ送信す

る。

【0027】したがって、この発明によれば、データ端末装置の現在位置を正確に検出することができる。その結果、データ端末装置は、データ端末装置の存在する地名に関連する暗号化コンテンツデータを正確に受信できる。

【0028】好ましくは、データ端末装置の制御部は、コンサート会場の位置を現在位置として送受信部を介して配信サーバへ送信し、コンサート会場で演奏されている曲と同じ暗号化音楽データを送受信部を介して受信する。

【0029】データ端末装置の制御部は、コンサート会場の位置を位置情報として配信サーバへ送信する。配信サーバは、位置情報に基づいてコンサート会場を抽出し、そのコンサート会場で演奏されている音楽データをデータ端末装置へ配信する。

【0030】したがって、この発明によれば、コンサート会場へ入れなくてもコンサート会場で演奏される音楽を聴くことができる。

【0031】好ましくは、データ端末装置の制御部は、コンサート会場の位置を配信サーバへ送信するとき、暗号化音楽データを再生するライセンスを通常料金よりも安い料金で受信する。

【0032】データ端末装置の制御部は、コンサート会場の位置を配信サーバへ送信し、配信サーバはコンサート会場で演奏されている暗号化音楽データと、その暗号化音楽データを再生するライセンスとをデータ端末装置へ送信するとき、通常の料金よりも安い料金をライセンスの配信に対して課金する。

【0033】したがって、ユーザは通用よりも安い料金で音楽データを受信して聴くことができる。

【0034】好ましくは、データ端末装置は、表示部をさらに備え、制御部は、現在位置に関連する画像データを送受信部を介して受信し、その受信した画像データを表示部に表示する。

【0035】データ端末装置の制御部は、データ端末装置の現在位置に関連する暗号化コンテンツデータとともに現在位置に関連する画像データを受信し、その受信した画像データを表示部に表示する。

【0036】したがって、この発明によれば、現在位置に関連する音楽データをその地方の景色を見ながら聴くことができる。

【0037】好ましくは、暗号化コンテンツデータは暗号化音楽データであり、データ端末装置は、暗号化音楽データを再生した音楽データを外部装置へ出力するための端子をさらに含み、制御部は、配信サーバにおいて再生された音楽データを受信し、その受信した音楽データを端子へ与え、音楽データの受信要求がキー操作部から入力されると配信サーバへ暗号化音楽データの配信要求を送信する。

10

20

30

40

50

【0038】データ端末装置の制御部は、配信サーバにおいて再生された音楽データを受信し、その受信した音楽データを外部装置へ出力するための端子に与える。そして、制御部は、外部装置へ出力した音楽データの受信要求がキー操作部から入力されると、配信サーバへ暗号化音楽データの配信要求を行なう。つまり、音楽データの試聴がなされ、最終的に音楽データの受信要求がデータ端末装置に入力されてから配信サーバへ暗号化コンテンツデータの配信要求がなされる。

【0039】したがって、この発明によれば、ユーザは 10 本当に聴きたい音楽データだけを受信して聴くことができる。

【0040】この発明によるデータ配信システムは、コンテンツデータを暗号化した暗号化コンテンツデータと、暗号化コンテンツデータを再生するライセンスとを保持する配信サーバと、配信サーバから暗号化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータおよびライセンスをデータ記録装置に記録および／または再生するデータ端末装置とを備え、配信サーバは、暗号化コンテンツデータの配信要求 20 を送信したデータ端末装置の現在位置に関連した暗号化コンテンツデータをデータ端末装置へ配信する。

【0041】この発明によるデータ配信システムにおいては、データ端末装置は暗号化コンテンツデータの配信要求を配信サーバへ行ない、配信サーバはデータ端末装置の現在位置に関連した暗号化コンテンツデータをデータ端末装置へ配信する。

【0042】したがって、この発明によれば、データ端末装置のユーザは、現在位置に関連する暗号化コンテンツデータを配信サーバから受信してコンテンツを再生す 30 ることができる。

【0043】好ましくは、配信サーバは、現在位置に関連した暗号化コンテンツデータの配信要求を受信すると、電話網によって位置情報を取得する位置情報センターから現在位置を受信する。

【0044】配信サーバは、データ端末装置から暗号化コンテンツデータの配信要求を受信すると、位置情報センターからデータ端末装置の現在位置を受信する。そして、配信サーバは、受信した現在位置に関連する暗号化コンテンツデータをデータ端末装置へ配信する。つまり、配信サーバは、データ端末装置が配信サーバへ暗号化コンテンツデータの配信要求を行なう経路と異なる経路からデータ端末装置の現在位置を取得する。

【0045】したがって、この発明によれば、データ端末装置が現在位置を検出する機能を備えていなくても、現在位置に関連した暗号化コンテンツデータを受信できる。

【0046】好ましくは、配信サーバは、データ端末装置からデータ現在位置を取得する。配信サーバは、暗号化コンテンツデータの配信要求とデータ端末装置の現在 50

位置とをデータ端末装置から受信する。

【0047】したがって、この発明によれば、データ端末装置の現在位置を正確に検知できる。

【0048】好ましくは、配信サーバは、携帯電話網を構成する基地局からデータ端末装置の現在位置を取得する。

【0049】配信サーバは、携帯電話網を構成する基地局からデータ端末装置の現在位置を取得する。

【0050】したがって、この発明によれば、データ端末装置が携帯電話網を介して配信サーバへアクセスすることにより、データ端末装置は現在位置を配信サーバへ送信しなくても、現在位置に関連する暗号化コンテンツデータを受信できる。

【0051】好ましくは、配信サーバは、現在位置を受信してからその現在位置に関連する暗号化コンテンツデータを検索し、その検索した暗号化コンテンツデータをデータ端末装置へ配信する。

【0052】配信サーバは、データ端末装置の現在位置を受信すると、現在位置に関連する暗号化コンテンツデータを検索し、データ端末装置へ配信する。

【0053】したがって、この発明によれば、配信サーバへ送信されるデータ端末装置の現在位置に応じた暗号化コンテンツデータをデータ端末装置へ配信できる。

【0054】好ましくは、配信サーバは、予め位置情報によって分類された暗号化コンテンツデータを保持し、現在位置を受信するとその現在位置に関連する暗号化コンテンツデータをデータ端末装置へ配信する。

【0055】配信サーバは、データ端末装置の現在位置を受信すると、その受信した現在位置に関連する暗号化コンテンツデータを予め分類した暗号化コンテンツデータから選択し、データ端末装置へ配信する。

【0056】したがって、この発明によれば、現在位置に関連する暗号化コンテンツデータを迅速にデータ端末装置へ配信できる。

【0057】好ましくは、配信サーバは、コンサート会場の位置を現在位置としてデータ端末装置から受信し、コンサート会場で演奏されている曲と同じ暗号化音楽データをデータ端末装置へ配信する。

【0058】配信サーバは、コンサート会場の位置を現在位置としてデータ端末装置から受信し、そのコンサート会場で演奏されている暗号化音楽データをデータ端末装置へ配信する。

【0059】したがって、この発明によれば、コンサート会場へ入れなくてもコンサート会場で演奏されている音楽を聴くことができる。

【0060】好ましくは、配信サーバは、暗号化音楽データを再生するライセンスを通常料金よりも安い料金でデータ端末装置へ配信する。

【0061】配信サーバは、データ端末装置の現在位置としてコンサート会場の位置を受信したとき、そのコン

サート会場で演奏されている暗号化音楽データを通常よりも安い料金でデータ端末装置で配信する。

【0062】したがって、ユーザは、通常よりも安い料金でコンサート会場で演奏されている音楽を聴くことができる。

【0063】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0064】図1は、本発明による携帯端末装置が再生の対象とする暗号化コンテンツデータをメモリカードへ配信するデータ配信システムの全体構成を概念的に説明するための概略図である。

【0065】なお、以下では携帯電話網を介してデジタル音楽データを各携帯電話ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画データ等を配信する場合においても適用することが可能なものである。

【0066】図1を参照して、配信キャリア20は、自己の携帯電話網を通じて得た、各携帯電話ユーザからの配信要求（配信リクエスト）をライセンスサーバに中継する。著作権の存在する音楽データを管理するライセンスサーバ10は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機100に装着されたメモリカード110が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア20である携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報としてライセンスを与える。

【0067】配信キャリア20は、自己の携帯電話網を通じて配信要求を送信した携帯電話機100に装着されたメモリカード110に対して、携帯電話網および携帯電話機100を介して暗号化コンテンツデータとライセンスとを配信する。

【0068】図1においては、たとえば携帯電話ユーザの携帯電話機100には、着脱可能なメモリカード110が装着される構成となっている。メモリカード110は、携帯電話機100により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機100中の音楽再生部（図示せず）に与える。

【0069】さらに、たとえば携帯電話ユーザは、携帯電話機100に接続したヘッドホン130等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【0070】以下では、このようなライセンスサーバ10と配信キャリア20とを併せて、配信サーバ30と総称することにする。

【0071】また、このような配信サーバ30から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

【0072】このような構成とすることで、まず、メモリカード110を利用しないと、配信サーバ30からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【0073】しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0074】図1に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話のユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信における暗号鍵を配信するための方式であり、また、第2には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第3には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【0075】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末（コンテンツを再生できるデータ再生端末を携帯電話機とも言う。以下同じ）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【0076】図2は、図1に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【0077】まず、配信サーバ30より配信されるデータについて説明する。Dataは、音楽データ等のコンテンツデータである。コンテンツデータDataには、ライセンス鍵Kcで復号可能な暗号化が施される。ライセンス鍵Kcによって復号可能な暗号化が施された暗号化コンテンツデータ {Data} Kcがこの形式で配信サーバ30より携帯電話ユーザに配布される。

【0078】なお、以下においては、{Y} Xという表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

【0079】さらに、配信サーバ30からは、暗号化コンテンツデータとともに、コンテンツデータに関する著

10

20

30

40

50

作権あるいはサーバアクセス関連等の平文情報としての付加情報Data-infが配布される。また、配信サーバ30からの暗号化コンテンツデータおよびライセンス鍵等の配信を特定するための管理コードであるトランザクションIDが配信サーバ30と携帯電話機100との間でやり取りされる。さらに、ライセンス情報としては、コンテンツデータDataを識別するためのコードであるコンテンツIDおよびライセンスの発行を特定できる管理コードであるライセンスIDや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ACに基づいて生成される、記録装置（メモリカード）のアクセスに対する制限に関する情報であるアクセス制限情報AC1およびデータ再生端末における制御情報である再生期限AC2等が存在する。以後、ライセンス鍵KcとコンテンツIDとライセンスIDと再生回数期限AC1と再生期限AC2とを併せて、ライセンスと総称することとする。

【0080】図3は、図1に示すデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する図である。

【0081】本発明の実施の形態においては、記録装置（メモリカード）やコンテンツデータを再生する携帯電話機のクラスごとに、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリストCRL(Class Revocation List)の運用を行なう。以下では、必要に応じて記号CRLによって禁止クラスリスト内のデータを表わすこともある。

【0082】禁止クラスリスト関連情報には、ライセンスの配信、および再生が禁止される携帯電話機およびメモリカードのクラスをリストアップした禁止クラスリストデータCRLが含まれる。

【0083】禁止クラスリストデータCRLは、配信サーバ30内で管理されるとともに、メモリカード内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には暗号化コンテンツデータおよび/またはライセンス鍵等のライセンスを配信する際の日時を基準として、携帯電話機から受取った禁止クラスリストの更新の有無を判断し、更新されていないとき、更新された禁止クラスリストを携帯電話機に配信する。また、禁止クラスリストの変更については、変更点のみを反映した差分データCRL_datを配信サーバ30側より発生して、これに応じてメモリカード内の禁止クラスリストCRLが書替えられる構成とするも可能である。また、禁止クラスリストのバージョンについては、CRL_verをメモリカード側より出力し、これを配信サーバ30側で確認することによってバージョン管理を実行する。差分データCRL_datには新たなバージョンの情報も含まれる。

【0084】このように、禁止クラスリストCRLを、配信サーバのみならずメモリカード内においても保持運用することによって、クラス固有すなわち、携帯電話機およびメモリカードの種類に固有の復号鍵が破られた、携帯電話機およびメモリカードへのライセンス鍵の供給を禁止する。このため、携帯電話機ではコンテンツデータの再生が、メモリカードではコンテンツデータの移動が行なえなくなる。

【0085】このように、メモリカード内の禁止クラスリストCRLは配信時に逐次データを更新する構成とする。また、メモリカード内における禁止クラスリストCRLの管理は、上位レベルとは独立にメモリカード内でタンパーレジスタントモジュール(Tamper Resistance Module)に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータCRLを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【0086】携帯電話機およびメモリカードには固有の公開暗号鍵Kp_pnおよびKp_mciがそれぞれ設けられ、公開暗号鍵Kp_pnおよびKp_mciは携帯電話機に固有の秘密復号鍵Kp_nおよびメモリカード固有の秘密復号鍵K_mciによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、携帯電話機の種類ごとおよびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称する。

【0087】また、データ再生端末（携帯電話機）およびメモリカードのクラス証明書として、Crt_fnおよびCmciがそれぞれ設けられる。これらのクラス証明書は、メモリカードおよびコンテンツ再生端末のクラスごとに異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が取得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

【0088】これらのメモリカードおよびコンテンツ再生端末固有の公開暗号鍵およびクラス証明書は、認証データ{Kp_mci//Cmci}Kp_maおよび{Kp_pn//Crt_fn}Kp_maの形式で、出荷時にメモリカードおよびデータ再生端末（携帯電話機）にそれぞれ記録される。後ほど詳細に説明するが、Kp_maは配信システム全体で共通の公開認証鍵である。

【0089】図4は、図1に示したデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する図である。

【0090】メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ30、携帯電話機100、およびメモリカード1

10において生成される共通鍵Ks1~Ks3が用いられる。

【0091】ここで、共通鍵Ks1~Ks3は、配信サーバ、携帯電話機もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ks1~Ks3を「セッションキー」とも呼ぶこととする。

【0092】これらのセッションキーKs1~Ks3は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモリカードによって管理される。具体的には、セッションキーKs1は、配信サーバによって配信セッションごとに発生される。セッションキーKs2は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキーKs3は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンス鍵等の送信を行なうことにより、セッションにおけるセキュリティ強度を向上させることができる。

【0093】また、メモリカード110内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵Kpmと、公開暗号鍵Kpmで暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵Kmが存在する。

【0094】図5は、図1に示したライセンスサーバ10の構成を示す概略ブロック図である。

【0095】ライセンスサーバ10は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンスID等の配信情報を保持するための情報データベース304と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース302と、禁止クラスリストCRLを管理するCRLデータベース306と、情報データベースに保持されたコンテンツデータのメニューを保持するメニューデータベース307と、コンテンツデータおよびライセンス鍵等の配信を特定するトランザクションIDを保持する配信記録データベース308と、情報データベース304、課金データベース302、CRLデータベース306、メニューデータベース307、および配信記録データベース308からのデータをバスBS1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

【0096】データ処理部310は、バスBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部315と、配信制御部315に制御され

て、配信セッション時にセッションキーKs1を発生するためのセッションキー発生部316と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ{Kpmci//Cmci} Kpmを復号するための公開認証鍵を保持する認証鍵保持部313と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ{Kpmci//Cmci} Kpmを通信装置350およびバスBS1を介して受けて、認証鍵保持部313からの公開認証鍵Kpmによって復号処理を行なう復号処理部312と、セッションキー発生部316により生成されたセッションキーKs1を復号処理部312によって得られた公開暗号鍵Kpmciを用いて暗号化して、バスBS1に出力するための暗号処理部318と、セッションキーKs1によって暗号化された上で送信されたデータをバスBS1より受けて、復号処理を行なう復号処理部320とを含む。

【0097】データ処理部310は、さらに、配信制御部315から与えられるライセンス鍵Kcおよび再生期限AC2を、復号処理部320によって得られたメモリカード固有の公開暗号鍵Kpmによって暗号化するための暗号処理部326と、暗号処理部326の出力を、復号処理部320から与えられるセッションキーKs2によってさらに暗号化してバスBS1に出力するための暗号処理部328とを含む。

【0098】ライセンスサーバ10の配信セッションにおける動作については、後ほどフローチャートを使用し

て詳細に説明する。

【0099】図6は、図1に示した携帯電話機100の構成を説明するための概略ブロック図である。

【0100】携帯電話機100は、携帯電話網により無線伝送される信号を受信するためのアンテナ1102と、アンテナ1102からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ1102に与えるための送受信部1104と、携帯電話機100の各部のデータ授受を行なうためのバスBS2と、バスBS2を介して携帯電話機100の動作を制御するためのコントローラ1106とを含む。

【0101】携帯電話機100は、さらに、外部からの指示を携帯電話機100に与えるためのキー操作部1108と、コントローラ1106等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ1110と、通常の通話動作において、バスBS2を介して与えられる受信データに基づいて音声再生するための音声再生部1112とを含む。

【0102】携帯電話機100は、さらに、音声再生部1112の出力をデジタル信号からアナログ信号に変換するDA変換器1113と、DA変換器1113の出力を外部出力装置等へ出力するための端子1114とを含む。

【0103】携帯電話機100は、さらに、通常の通話動作において、携帯電話機100のユーザが話した音声信号を入力するマイク1115と、マイク1115からの音声信号をアナログ信号からデジタル信号に変換するAD変換器1116と、AD変換器1116からのデジタル信号を所定の方式に従って符号化してバスBS2へ与える音声符号化部1117とを含む。

【0104】携帯電話機100は、さらに、配信サーバ30からのコンテンツデータ（音楽データ）を記憶しつつ復号化処理を行なうための着脱可能なメモリカード110と、メモリカード110とバスBS2との間のデータの授受を制御するためのメモリインタフェース1200とを含む。

【0105】携帯電話機100は、さらに、携帯電話機の種類（クラス）ごとにそれぞれ設定される、公開暗号鍵Kp1およびクラス証明書Crtf1を公開復号鍵Kpmaで復号することでその正当性を認証できる状態に暗号化した認証データ{Kp1/Crtf1}Kpmaを保持する認証データ保持部1202を含む。ここで、携帯電話機（データ端末装置）100のクラスn

【0106】携帯電話機100は、さらに、携帯電話機（コンテンツ再生回路）固有の復号鍵であるKp1を保持するKp1保持部1204と、バスBS2から受けたデータをKp1によって復号しメモリカード110によって発生されたセッションキーKs2を得る復号処理部1206とを含む。

【0107】携帯電話機100は、さらに、メモリカード110に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード110との間でバスBS2上においてやり取りされるデータを暗号化するためのセッションキーKs3を乱数等により発生するセッションキー発生部1210と、発生されたセッションキーKs3を復号処理部1206によって得られたセッションキーKs2によって暗号化しバスBS2に出力する暗号処理部1208とを含む。

【0108】携帯電話機100は、さらに、バスBS2上のデータをセッションキーKs3によって復号して出力する復号処理部1212と、バスBS2より暗号化コンテンツデータ{Data}Kcを受けて、復号処理部1212より取得したライセンス鍵Kcによって復号しコンテンツデータを出力する復号処理部1214と、復号処理部1214の出力を受けてコンテンツデータを再生するための音楽再生部1216と、音楽再生部1216の出力をデジタル信号からアナログ信号に変換するDA変換器1218とを含む。

【0109】携帯電話機100は、さらに、DA変換器1113とDA変換器1218との出力を受けて、動作モードに応じて選択的に端子1114または端子1220から出力するためのスイッチ1222と、スイッチ1

222の出力を受けて、ヘッドホーン130と接続するための接続端子1224と、携帯電話機100の現在位置を検出する位置検出部1226とを含む。

【0110】ここで、位置検出部1226は、GPSによって携帯電話機100の現在位置を検出する。GPSを用いることによって、携帯電話機100は、約100mの精度で現在位置を特定することができる。

【0111】また、位置検出部1226は、相対測位方式（ディファレンシャルGPS（Differential GPS））によって携帯電話機100の現在位置を検出してもよい。この、相対測位方式とは、基準点の位置とGPSによって検出した携帯電話機100の位置とを照合比較して衛星系、伝搬系等による誤差を除去して精度の高い位置を検出する方式である。

【0112】なお、図6においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【0113】携帯電話機100の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0114】図7は、メモリカード110の構成を説明するための概略ブロック図である。既に説明したように、メモリカードに固有の公開暗号鍵および秘密復号鍵として、KpmciおよびKmc iが設けられ、メモリカードのクラス証明書Cmciが設けられるが、メモリカード110においては、これらは自然数i=1でそれぞれ表わされるものとする。

【0115】したがって、メモリカード110は、認証データ{Kpmc1/Cmci}Kpmaを保持する認証データ保持部1400と、メモリカードの種類ごとに設定される固有の復号鍵であるKmc1を保持するKmc1保持部1402と、メモリカードごとに固有に設定される秘密復号鍵Km1を保持するKm1保持部1421と、Km1によって復号可能な公開暗号鍵Kpm1を保持するKpm1保持部1416とを含む。認証データ保持部1400は、メモリカードの種類およびクラスごとにそれぞれ設定される秘密暗号鍵Kpmc1およびクラス証明書Cmciを公開認証鍵Kpmaで復号することでその正当性を認証できる状態に暗号化した認証データ{Kpmc1/Cmci}Kpmaとして保持する。

【0116】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【0117】メモリカード110は、さらに、メモリインタフェース1200との間で信号を端子1201を介

して授受するインタフェース1423と、インタフェース1423との間で信号をやり取りするバスBS3と、バスBS3にインタフェース1423から与えられるデータから、メモ리카ードの種類ごとに固有の秘密復号鍵Kmc1をKmc1保持部1402から受けて、配信サーバ30が配信セッションにおいて生成したセッションキーKs1を接点Paに出力する復号処理部1404と、KPma保持部1414から認証鍵KPmaを受けて、バスBS3に与えられるデータからKPmaによる復号処理を実行して復号結果を暗号処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1444によって選択的に与えられるデータを暗号化してバスBS3に出力する暗号処理部1406とを含む。

【0118】メモ리카ード110は、さらに、配信、および再生の各セッションにおいてセッションキーKs2を発生するセッションキー発生部1418と、セッションキー発生部1418の出力したセッションキーKs2を復号処理部1408によって得られる公開暗号鍵KPpnもしくはKPmciによって暗号化してバスBS3に送出する暗号処理部1410と、バスBS3よりセッションキーKs2によって暗号化されたデータを受けてセッションキー発生部1418より得たセッションキーKs2によって復号し、復号結果をバスBS4に送出する復号処理部1412とを含む。

【0119】メモ리카ード110は、さらに、バスBS3上のデータを公開暗号鍵KPm1と対をなすメモ리카ード110固有の秘密復号鍵Km1によって復号するための復号処理部1422と、禁止クラスリストのバージョン更新のためのデータCRL_datによって逐次更新される禁止クラスリストデータCRLをバスBS4より受けて格納するとともに、暗号化コンテンツデータ

{Data} Kcおよび付加情報Data-infをバスBS3より受けて格納するためのメモリ1415とを含む。メモリ1415は、例えば半導体メモリによって構成される。また、メモリ1415は、禁止クラスリストCRLを記録したCRL領域1415Aと、コンテンツIDを含むHeader、暗号化コンテンツデータ

{Data} Kc、および暗号化コンテンツデータの関連情報Data-infを記録したデータ領域1415Bとから成る。

【0120】メモ리카ード110は、さらに、復号処理部1422によって得られるライセンスを保持するためのライセンス情報保持部1440と、バスBS3を介して外部との間でデータ授受を行ない、バスBS4との間で再生情報等を受けて、メモ리카ード110の動作を制御するためのコントローラ1420とを含む。

【0121】ライセンス情報保持部1440は、N個(N:自然数)のバンクを有し、各ライセンスに対応するライセンスをバンクごとに保持する。

【0122】なお、図7において、実線で囲んだ領域は、メモ리카ード110内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタンスモジュール(Tamper Resistance Module)である。

【0123】もちろん、メモリ1415も含めて、モジュールTRM内に組込まれる構成としてもよい。しかしながら、図7に示したような構成とすることで、メモリ1415中に保持されている再生に必要な再生情報は、いずれも暗号化されているデータであるため、第三者はこのメモリ1415中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ1415を設ける必要がないので、製造コストが低減されるという利点がある。

【0124】図8～図11は、図1に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生する配信動作(以下、配信セッションともいう)を説明するための第1～第4のフローチャートである。

【0125】図8を参照して、携帯電話機100のユーザからキー操作部1108を介してコンテンツデータの配信要求がなされると、携帯電話機100は、メニューの送信要求を配信サーバ30へ送信する(ステップS70)。配信サーバ30の配信制御部315は、通信装置350およびバスBS1を介してメニューの送信要求を受信すると(ステップS72)、メニューデータベース307からバスBS1を介してメニューを読み出し、その読み出したメニューをバスBS1および通信装置350を介して携帯電話機100へ送信する(ステップS74)。携帯電話機110は、送受信部1104によってメニューを受信し、コントローラ1106は、メニューを表示部1110に表示する(ステップS76)。

【0126】そうすると、携帯電話機100の表示部1110には、図12に示すメニュー61が表示される。ユーザは、メニュー61の選択番号1, 2, 3, ...を選択することによって配信を希望する暗号化コンテンツデータのジャンルを選択する。表示部1110には、別の画面に移行するための移行部1111が設けられている。ユーザは、表示部1110に表示されたメニュー61から希望する暗号化コンテンツデータのジャンルを選択すると、移行部1111をクリックする。

【0127】携帯電話機100のコントローラ1106は、ジャンルが選択された否かを判断する(ステップS78)。選択すべきジャンルが存在しないときはステップS170へ移行し、配信動作は終了する。ジャンルが選択され、移行部1111をクリックされると、コントローラ1106は、選択されたジャンルに含まれるアド

レスを送受信部1104を介して配信サーバ30へ送信し、選択されたジャンルの画面を送信するように要求する(ステップS80)。メニュー61から「地域関連」のジャンルが選択されると、携帯電話機100のコントローラ1106は、地域関連のアドレスを送受信部1104を介して配信サーバ30へ送信する。

【0128】配信サーバ30の配信制御部315は、通信装置350およびバスBS1を介してジャンルメニューの送信要求を受信すると(ステップS81)、メニューデータベース307からバスBS1を介して要求されたジャンルメニューを読み出し、その読み出したジャンルメニューをバスBS1および通信装置350を介して携帯電話機100へ送信する(ステップS82)。地域関連のジャンルを要求された場合、配信制御部315は、地域関連のジャンルに含まれるメニューをメニューデータベース307から読み出し、バスBS1および通信装置350を介して携帯電話機100へ送信する。

【0129】携帯電話機110は、送受信部1104によってジャンルメニューを受信し、コントローラ1106は、ジャンルメニューを表示部1110に表示する(ステップS83)。そうすると、携帯電話機100の表示部1110には、図12に示すジャンルメニュー62が表示される。ユーザは、ジャンルメニュー62の選択番号1, 2, 3, ...を選択することによって配信を希望する暗号化コンテンツデータの項目を選択する。ユーザが選択した地域関連のジャンルメニュー62は、曲名、歌詞、出身歌手、出身作曲者等から成る。地域関連のジャンルメニュー62に含まれる曲名、歌詞、出身歌手、出身作曲者等は、携帯電話機100の現在位置の地名を含む曲名、歌詞、その地名を出身地とする歌手、作曲者等を表す。たとえば、携帯電話機100の現在位置が東京であるならば、曲名に「東京」を含む音楽データを意味する。この地名の範囲は、そう狭い地域を指すのではなく、おおむね都道府県程度である。

【0130】ユーザは、ディスプレイ1110を見て表示された地域関連のジャンルメニュー62から希望する項目を選択し、移行部1111をクリックする。携帯電話機100のコントローラ1106は、項目が選択された否かを判断する(ステップS84)。選択すべき項目が存在しないときはステップS170へ移行し、配信動作は終了する。項目が選択され、移行部1111がクリックされると、コントローラ1106は、選択された項目に含まれるアドレスを送受信部1104を介して配信サーバ30へ送信し、選択された項目の画面を送信するように要求するとともに、位置検出部1226がGPSによって検出した携帯電話機100の現在位置を送信する(ステップS85)。ジャンルメニュー62から「曲名」の項目が選択されると、携帯電話機100のコントローラ1106は、曲名のアドレスを送受信部1104を介して配信サーバ30へ送信する。

【0131】配信サーバ30の配信制御部315は、通信装置350およびバスBS1を介して項目メニューの送信要求および携帯電話機100の現在位置を受信する(ステップS86)。そして、配信制御部315は、バスBS1を介して情報データベース304から携帯電話機100の現在位置が所在する地名を曲名に含む音楽データを検索し、その曲名リストを読み出し、バスBS1および通信装置350を介して携帯電話機100へ送信する(ステップS87)。携帯電話機100の現在位置が所在する地名が東京であるならば、配信制御部315は、東京を曲名に含む音楽データの曲名リストを携帯電話機100に送信する。

【0132】携帯電話機100のコントローラ1106は、送受信部1104を介して曲名リストを受信し、ディスプレイ1110に曲名リスト63を表示する(ステップS83)。ユーザは、ディスプレイ1110に表示された曲名リスト63を見て表示された曲名リスト63から希望する曲を選択する。

【0133】携帯電話機100のコントローラ1106は、曲名が選択された否かを判断する(ステップS89)。選択すべき曲名がないときは、ステップS170へ移行し、配信動作は終了する。

【0134】曲名リスト63は、暗号化コンテンツデータを特定するためのコンテンツIDを含んでおり、ステップS89において暗号化コンテンツデータが選択されたとき、曲名リスト63から選択された暗号化コンテンツデータのコンテンツIDが抽出される(ステップS90)。そして、キー操作部1108を介して暗号化コンテンツデータのライセンスを購入するための購入条件ACが入力される(ステップS91)。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Kcを購入するために、暗号化コンテンツデータの再生回数制限AC1、および再生期限AC2を設定して購入条件ACが入力される。

【0135】他のジャンル、および項目が選択されたときも、上記と同じ方法によって選択されたジャンル、および項目が配信サーバ30から携帯電話機100に送信され、最終的に、ユーザが希望する暗号化コンテンツデータが特定される。

【0136】また、曲名リスト63から暗号化音楽データを最終的に決定するとき、配信サーバ30と接続した状態で、配信サーバ30で再生された音楽データを携帯電話機100が受信し、ユーザが試聴した後に配信を希望する暗号化音楽データを最終的に決定するようにしても良い。

【0137】次に、図9を参照して、携帯電話機100は、ユーザが暗号化コンテンツデータを選択することによって抽出したコンテンツID(ステップS90参照)の指定による配信リクエストがなされる(ステップS100)。

【0138】メモリカード110においては、この配信リクエストに応じて、認証データ保持部1400より認証データ {K P m c 1 / / C m c 1} K P m a が出力される (ステップS102)。

【0139】携帯電話機100は、メモリカード110からの認証のための認証データ {K P m c 1 / / C m c 1} K P m a に加えて、コンテンツID、ライセンス購入条件のデータACとを配信サーバ30に対して送信する (ステップS104)。

【0140】配信サーバ30では、携帯電話機100からコンテンツID、認証データ {K P m c 1 / / C m c 1} K P m a、ライセンス購入条件のデータACを受信し (ステップS106)、復号処理部312においてメモリカード110から出力された認証データを公開認証鍵K P m a で復号処理を実行する (ステップS108)。

【0141】配信制御部315は、復号処理部312における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード110が正規のメモリカードからの公開暗号鍵K P m c 1と証明書C m c 1を保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう (ステップS110)。正当な認証データであると判断された場合、配信制御部315は、公開暗号鍵K P m c 1および証明書C m c 1を承認し、受理する。そして、次の処理 (ステップS112) へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵K P m c 1および証明書C m c 1を受理しないで処理を終了する (ステップS170)。

【0142】認証の結果、正規の機器であることが認識されると、配信制御部315は、次に、メモリカード110のクラス証明書C m c 1が禁止クラスリストC R L にリストアップされているかどうかをC R L データベース306に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する (ステップS170)。

【0143】一方、メモリカード110のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する (ステップS112)。

【0144】認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ30において、配信制御部315は、配信を特定するための管理コードであるトランザクションIDを生成する (ステップS113)。また、セッションキー発生部316は、配信のためのセッションキーK s 1を生成する。セッションキーK s 1は、復号処理部312によって得られたメモリカード110に対応する公開暗号鍵K P m c 1によって、暗号処理部318に

よって暗号化される (ステップS114)。

【0145】トランザクションIDおよび暗号化されたセッションキーK s 1は、トランザクションID / / {K s 1} K m c 1として、バスB S 1および通信装置350を介して外部に出力される (ステップS116)。

【0146】携帯電話機100が、トランザクションID / / {K s 1} K m c 1を受信すると (ステップS118)、メモリカード110においては、メモリインタフェース1200を介して、バスB S 3に与えられた受信データを、復号処理部1404が、保持部1402に保持されるメモリカード110固有の秘密復号鍵K m c 1により復号処理することにより、セッションキーK s 1を復号し抽出する (ステップS120)。

【0147】コントローラ1420は、配信サーバ30で生成されたセッションキーK s 1の受理を確認すると、セッションキー発生部1418に対して、メモリカード110において配信動作時に生成されるセッションキーK s 2の生成を指示する。

【0148】また、配信セッションにおいては、コントローラ1420は、メモリカード110内のメモリ1415に記録されている禁止クラスリストのデータC R L _ d a t をメモリ1415から抽出してバスB S 4に出力する。

【0149】暗号処理部1406は、切換スイッチ1442の接点P a を介して復号処理部1404より与えられるセッションキーK s 1によって、切換スイッチ1444および1446の接点を順次切換えることによって与えられるセッションキーK s 2、公開暗号鍵K P m 1および禁止クラスリストのデータC R L _ d a t を1つのデータ列として暗号化して、{K s 2 / / K P m 1 / / C R L _ d a t} K s 1をバスB S 3に出力する (ステップS122)。

【0150】バスB S 3に出力された暗号化データ {K s 2 / / K P m 1 / / C R L _ v e r} K s 1は、バスB S 3からインタフェース1423、端子1201およびメモリインタフェース1200を介して携帯電話機100に出力され、携帯電話機100から配信サーバ30に送信される (ステップS124)。

【0151】配信サーバ30は、トランザクションID / / {K s 2 / / K P m 1 / / C R L _ d a t} K s 1を受信して、復号処理部320においてセッションキーK s 1による復号処理を実行し、メモリカード110で生成されたセッションキーK s 2、メモリカード110固有の公開暗号鍵K P m 1およびメモリカード110における禁止クラスリストのデータC R L _ d a t を受理する (ステップS126)。

【0152】配信制御部315は、ステップS106で取得したコンテンツIDおよびライセンス購入条件のデータACに従って、ライセンスID、アクセス制限情報

AC1および再生期限AC2を生成する(ステップS128)。さらに、暗号化コンテンツデータを復号するためのライセンス鍵Kcを情報データベース304より取得する(ステップS130)。

【0153】配信制御部315は、生成したライセンス、すなわち、ライセンス鍵Kc、再生期限AC2、ライセンスID、コンテンツID、およびアクセス制限情報AC1を暗号処理部326に与える。暗号処理部326は、復号処理部320によって得られたメモリカード110固有の公開暗号鍵Kpm1によってライセンスを暗号化する(ステップS132)図10を参照して、配信サーバ30において、メモリカード110から送信された禁止クラスリストのデータCRL_datが最新か否かが判断され、データCRL_datが最新と判断されたとき、ステップS134へ移行する。また、データCRL_datが最新でないときはステップS137へ移行する(ステップS133)。

【0154】データCRL_datが最新と判断されたとき、暗号処理部328は、暗号処理部326から出力された暗号化データ{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1をメモリカード110において発生されたセッションキーKs2によって暗号化を行い、暗号化データ{[Kc//AC2//ライセンスID//コンテンツID//AC1]Km1}Ks2をバスBS1に出力する。そして、配信制御部315は、バスBS1上の暗号化データ{[Kc//AC2//ライセンスID//コンテンツID//AC1]Km1}Ks2を通信装置350を介して携帯電話機100へ送信する(ステップS134)。

【0155】そして、携帯電話機100は、暗号化データ{[Kc//AC2//ライセンスID//コンテンツID//AC1]Km1}Ks2を受信し(ステップS135)、バスBS2およびメモリインタフェース1200を介してメモリカード110へ送信する。メモリカード110の復号処理部1412は、暗号化データ{[Kc//AC2//ライセンスID//コンテンツID//AC1]Km1}Ks2を端子1201およびインタフェース1423を介して受取り、セッションキー発生部1418によって発生されたセッションキーKs2によって復号し、{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1を受理する(ステップS136)。その後、ステップS146へ移行する。

【0156】一方、配信サーバ30において、CRL_datが最新でないと判断されると、配信制御部315は、バスBS1を介してCRLデータベース306から最新の禁止クラスリストのデータCRL_datを取得する(ステップS137)。

【0157】暗号処理部328は、暗号処理部326の出力と、配信制御部315がバスBS1を介して供給す

る禁止クラスリストの最新データCRL_datとを受けて、メモリカード110において生成されたセッションキーKs2によって暗号化する。暗号処理部328より出力された暗号化データは、バスBS1および通信装置350を介して携帯電話機100に送信される(ステップS138)。

【0158】このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【0159】携帯電話機100は、送信された暗号化データ{[Kc//AC2//ライセンスID//コンテンツID//AC1]Km1//CRL_dat}Ks2を受信し(ステップS140)、メモリインタフェース1200を介してメモリカード110へ出力する。メモリカード110においては、端子1201およびインタフェース1423を介して、バスBS3に与えられた受信データを復号処理部1412によって復号する。復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2を用いてバスBS3の受信データを復号しバスBS4に出力する(ステップS142)。

【0160】この段階で、バスBS4には、Km1保持部1421に保持される秘密復号鍵Km1で復号可能な暗号化ライセンス{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1と、CRL_datとが出力される(ステップS142)。コントローラ1420の指示によって受理した最新の禁止クラスリストCRL_datによってメモリ1415内の禁止クラスリストCRLが書き換えられる(ステップS144)。

【0161】ステップS134、S135、S136は、メモリカード110から送られてきた禁止クラスリストCRL_datが最新の場合のライセンス鍵Kc等のメモリカード110への配信動作であり、ステップS137、S138、S140、S142、S144は、メモリカード110から送られてきた禁止クラスリストCRL_datが最新でない場合のライセンス鍵Kc等のメモリカード110への配信動作である。このように、メモリカード110から送られてきた禁止クラスリストCRL_datが更新されているか否かを、逐一、確認し、更新されていないとき、最新の禁止クラスリストCRL_datをCRLデータベース306から取得し、メモリカード110に配信することによって、ライセンスの破られたメモリカードへの暗号化コンテンツデータ{Data}Kcの配信を防止し、かつ、ライセンスの破られた携帯電話機による暗号化コンテンツデータ

10

20

30

40

50

{Data} Kcの再生を防止できる。

【0162】ステップS136またはステップS144の後、コントローラ1420の指示によって、暗号化ライセンス {Kc//AC2//ライセンスID//コンテンツID//AC1} Km1は、復号処理部1422において、秘密復号鍵Km1によって復号され、ライセンス (ライセンス鍵Kc、ライセンスID、コンテンツID、再生回数制限AC1および再生期限AC2) が受理される (ステップS148)。

【0163】コントローラ1420は、ライセンスをライ
10 センス情報保持部1440に記録する (ステップS150)。

【0164】図11を参照して、携帯電話機100のコントローラ1106は、ステップS88およびステップS94において立てたフラグを参照し、配信サーバ30から暗号化コンテンツデータを取得するか否かを判断する。そして、暗号化コンテンツデータを配信サーバ30から取得しないとき、ステップS164へ移行し、暗号化コンテンツデータを配信サーバ30から取得するとき、ステップS154へ移行する。

【0165】暗号化コンテンツデータを配信サーバ30から取得するとき、携帯電話機100は、配信サーバ30から送られたトランザクションIDと、暗号化コンテンツデータの配信要求を配信サーバ30へ送信する (ステップS154)。

【0166】配信サーバ30は、トランザクションIDおよび暗号化コンテンツデータの配信要求を受信し (ステップS156)、情報データベース304より、暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infを取得して、これらのデータをバスBS
30 1および通信装置350を介して出力する (ステップS158)。

【0167】携帯電話機100は、{Data} Kc//Data-infを受信して、暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infを受理する (ステップS160)。暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infは、メモリインタフェース1200、端子1201、およびインタフェース1423を介してメモリカード110のバスBS3に伝達される。メモリカード110においては、受信した暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infがそのままメモリ1415に記録される (ステップS162)。

【0168】そして、ステップS152において暗号化コンテンツデータを配信サーバ30から受信しないと判断されたときも含め、メモリカード110から配信サーバ30へは、トランザクションID//配信受理の通知が送信され (ステップS164)、配信サーバ30でトランザクションID//配信受理を受信すると (ステップS166)、課金データベース302への課金データ
50

の格納、およびトランザクションIDの配信記録データベース308への記録が行われて配信終了の処理が実行され (ステップS168)、全体の処理が終了する (ステップS170)。

【0169】このようにして、携帯電話機100に装着されたメモリカード110が正規の機器であること、同時に、クラス証明書Cmc1とともに暗号化して送信してきた公開暗号鍵Kp1およびKmc1が有効であることを確認した上で、それぞれのクラス証明書Cmc1が禁止クラスリスト、すなわち、公開暗号鍵Kp1およびKmc1による暗号化が破られたクラス証明書リストに記載されていないメモリカードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモリカードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【0170】また、配信サーバ30への暗号化コンテンツデータ {Data} Kcの配信要求時にメモリカード110における暗号化コンテンツデータ {Data} Kc、ライセンス鍵Kc、および再生回数制限AC1等の
20 記録状況に応じて、必要な配信だけを配信サーバ30に要求することができる。その結果、無駄な配信を防止することができる。

【0171】次に、図13および図14を参照してメモリカード110に配信されたコンテンツデータの携帯電話機100における再生動作について説明する。図13を参照して、再生動作の開始とともに、携帯電話機100のユーザからキー操作部1108を介して再生指示が携帯電話機100にインプットされる (ステップS200)。そうすると、コントローラ1106は、バスBS
30 2を介して認証データ保持部1202から認証データ {Kp1//Crtf1} KPmaを読み出し、メモリインタフェース1200を介してメモリカード110へ認証データ {Kp1//Crtf1} KPmaを入力する (ステップS201)。

【0172】そうすると、メモリカード110は、認証データ {Kp1//Crtf1} KPmaを受理する (ステップS202)。そして、メモリカード110の復号処理部1408は、受理した認証データ {Kp1//Crtf1} KPmaを、KPma保持部1414
40 に保持された公開認証鍵KPmaによって復号し (ステップS203)、コントローラ1420は復号処理部1408における復号処理結果から、認証処理を行なう。すなわち、認証データ {Kp1//Crtf1} KPmaが正規の認証データであるか否かを判断する認証処理を行なう (ステップS204)。復号できなかった場合、コントローラ1420は認証データ不受理の出力をデータBS3および端子1201を介して携帯電話機100のメモリインタフェース1200へ出力する (ステップS206)。認証データが復号できた場合、コント
50 ローラ1420は、取得した証明書Crtf1がメモリ

1415から読出した禁止クラスリストデータに含まれるか否かを判断する(ステップS205)。この場合、証明書Crtf1にはIDが付与されており、コントローラ1420は、受理した証明書Crtf1のIDが禁止クラスリストデータの中に存在するか否かを判別する。証明書Crtf1が禁止クラスリストデータに含まれると判断されると、コントローラ1420は認証データ不受理の出力をデータBS3および端子1201を介して携帯電話機100のメモリインタフェース1200へ出力する(ステップS206)。

【0173】ステップS204において認証データが公開認証鍵Kpmaで復号できなかったとき、およびステップS205において受理した証明書Crtf1が禁止クラスリストデータに含まれているとき、認証データ不受理の出力がなされる。そして、携帯電話機100のコントローラ1106は、メモリインタフェース1200を介して認証データ不受理の出力を受けると、認証データ不受理のデータをディスプレイ1110に表示する(ステップS207)。

【0174】ステップS205において、証明書Crtf1が禁止クラスリストデータに含まれていないと判断されると、図14を参照して、メモリカード110のセッションキー発生部1418は、再生セッション用のセッションキーKs2を発生させる(ステップS208)。そして、暗号処理部1410は、セッションキー発生部1418からのセッションキーKs2を、復号処理部1408で復号された公開暗号鍵Kp1によって暗号化した{Ks2}Kp1をバスBS3へ出力する(ステップS209)。そうすると、コントローラ1420は、端子1201を介してメモリインタフェース1200へ{Ks2}Kp1を出力し、携帯電話機100のコントローラ1106は、メモリインタフェース1200を介して{Ks2}Kp1を取得する。そして、Kp1保持部1204は、秘密復号鍵Kp1を復号処理部1206へ出力する。

【0175】復号処理部1206は、Kp1保持部1204から出力された、公開暗号鍵Kp1と対になっている秘密復号鍵Kp1によって{Ks2}Kp1を復号し、セッションキーKs2を暗号処理部1208へ出力する(ステップS210)。そうすると、セッションキー発生部1210は、再生セッション用のセッションキーKs3を発生させ、セッションキーKs3を暗号処理部1208へ出力する(ステップS211)。暗号処理部1208は、セッションキー発生部1210からのセッションキーKs3を復号処理部1206からのセッションキーKs2によって暗号化して{Ks3}Ks2を出力し、コントローラ1106は、バスBS2およびメモリインタフェース1200を介して{Ks3}Ks2をメモリカード110へ出力する(ステップS212)。

【0176】メモリカード110の復号処理部1412は、端子1201、インタフェース1423、およびバスBS3を介して{Ks3}Ks2を入力し、セッションキー発生部1418によって発生されたセッションキーKs2によって{Ks3}Ks2を復号して、携帯電話機100で発生されたセッションキーKs3を取得する(ステップS213)。

【0177】セッションキーKs3の受理に応じて、コントローラ1420は、ライセンス情報保持部1440内の対応するアクセス制限情報AC1を確認する(ステップS214)。

【0178】ステップS214においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報AC1を確認することにより、既に再生不可の状態である場合には再生動作を終了し、再生回数制限に制限がある場合にはアクセス制限情報AC1のデータを更新し再生可能回数を更新した後に次のステップに進む(ステップS215)。一方、アクセス制限情報AC1によって再生回数制限が制限されていない場合においては、ステップS215はスキップされ、再生回数制限AC1は更新されることなく処理が次のステップ(ステップS216)に進行される。

【0179】また、ライセンス情報保持部1440内にリクエスト曲の当該コンテンツIDが存在しない場合においても、再生不可の状態にあると判断して、再生動作を終了する。

【0180】ステップS214において、当該再生動作において再生が可能であると判断された場合には、ライセンス情報保持部1440に記録された再生リクエスト曲のライセンス鍵Kcおよび再生期限AC2がバスBS4上に出力される(ステップS216)。

【0181】得られたライセンス鍵Kcと再生期限AC2は、切換スイッチ1444の接点Pdを介して暗号処理部1406に送られる。暗号処理部1406は、切換スイッチ1442の接点Pdを介して復号処理部1412より受けたセッションキーKs3によってバスBS4から受けたライセンス鍵Kcと再生期限AC2とを暗号化し、{Kc//AC2}Ks3をバスBS3に出力する(ステップS217)。

【0182】バスBS3に出力された暗号化データは、インタフェース1423、端子1202、およびメモリインタフェース1200を介して携帯電話機100に送出される。

【0183】携帯電話機100においては、メモリインタフェース1200を介してバスBS2に伝達される暗号化データ{Kc//AC2}Ks3を復号処理部1212によって復号処理を行ない、ライセンス鍵Kcおよび再生期限AC2を受理する(ステップS218)。復号処理部1212は、ライセンス鍵Kcを復号処理部1214に伝達し、再生期限AC2をバスBS2に出力す

る。

【0184】コントローラ1106は、バスBS2を介して、再生期限AC2を受信して再生の可否の確認を行なう(ステップS219)。

【0185】ステップS219においては、再生期限AC2によって再生不可と判断される場合には、再生動作は終了される。

【0186】ステップS219において再生可能と判断された場合、コントローラ1106は、メモリインタフェース1200を介してメモリカード110に暗号化コンテンツデータ {Data} Kcを要求する。そうすると、メモリカード110のコントローラ1420は、メモリ1415から暗号化コンテンツデータ {Data} Kcを取得し、バスBS3および端子1201を介してメモリインタフェース1200へ出力する(ステップS220)。

【0187】携帯電話機100のコントローラ1106は、メモリインタフェース1200を介して暗号化コンテンツデータ {Data} Kcを取得し、バスBS2を介して暗号化コンテンツデータ {Data} Kcを復号処理部1214へ与える。そして、復号処理部1214は、暗号化コンテンツデータ {Data} Kcを復号処理部1212から出力されたコンテンツ鍵Kcによって復号してコンテンツデータDataを取得する(ステップS221)。

【0188】そして、復号されたコンテンツデータDataは音楽再生部1216へ出力され、音楽再生部1216は、コンテンツデータを再生し、DA変換器1218はデジタル信号をアナログ信号に変換して端子1220へ出力する。そして、スイッチ1222は端子1220を選択して音楽データは端子1224を介してヘッドホン130へ出力されて再生される(ステップS222)。これによって再生動作が終了する。

【0189】上記においては、携帯電話機100は、現在位置をGPSによって検出し、その検出した現在位置を配信サーバ30へ送信するとして説明したが、本発明においては、これに限らず、配信サーバ30は、他の方法によって携帯電話機100の現在位置を取得しても良い。すなわち、配信サーバ30は、図15に示す位置情報センター40から携帯電話機100の現在位置を取得しても良い。配信サーバ30は、位置情報センター40と接続されている。位置情報センター40は、地図データベース41、基地局データベース42、および端末機位置データ43を含む。位置情報センター40は、電話網50と接続されており、電話網50は、公衆回線網51と、基地局52～54とを含む。

【0190】配信サーバ30は、携帯電話機100から暗号化コンテンツデータの配信要求を受信すると、位置情報センター40に携帯電話機100の現在位置を要求する。そうすると、位置情報センター40は、基地局5

2～54の基地局データを電話網50に要求する。基地局52～54は、公衆回線網51を介して基地局データの要求を受取り、携帯電話機100に基地局データを要求する。

【0191】携帯電話機100は、基地局コードと電界強度情報とを基地局52～54へ送信する。そして、基地局52～54は、基地局コードと電界強度情報とを公衆回線網51を介して位置情報センター40へ送信する。位置情報センター40は、受信した基地局コードに基づいて基地局データベース42を検索し、基地局コードと電界強度情報とを送信してきた3つの基地局の所在地を抽出する。また、位置情報センター40は、受信した電界強度情報に基づいて、携帯電話機100が3つの基地局52～54からどの程度離れているかを計算する。そして、位置情報センター40は、3つの基地局の所在地、および3つの基地局からの距離に基づいて、地図データベース41を参照して携帯電話機100の現在位置を割出し、その割出した現在位置を配信サーバ30へ送信するとともに端末機位置データベース43に記憶する。

【0192】これによって、配信サーバ30は、暗号化コンテンツデータの配信を要求した携帯電話機100の現在位置を検知することができる。

【0193】携帯電話機100が配信サーバ30へ携帯電話網を介して暗号化コンテンツデータの配信を要求するので、携帯電話機100は暗号化コンテンツデータの配信要求と同時に基地局コードを配信サーバへ送信するようにしても良い。配信サーバ30は、基地局コードに対応する地名データベースを保持しており、受信した基地局コードに基づいて携帯電話機100の現在位置が所在する地名を割出すことができる。本発明において要求される現在位置に関する位置情報は、都道府県レベルの位置情報でよいので、配信サーバ30は基地局コードに基づいて位置情報を得ることができる。

【0194】また、本発明においては、コンサート会場近くで配信サーバ30へ暗号化コンテンツデータの配信要求を行なったとき、そのコンサート会場で演奏されている音楽データを携帯電話機100へ送信するようにしても良い。携帯電話機100の現在位置の検出方法は上述したのと同じ方法である。この場合、配信サーバ30は、配信要求された暗号化コンテンツデータのライセンスを携帯電話機100へ送信する際、通常よりも安い料金を課金する。これによって、コンサート会場に入れなくても、コンサート会場で演奏されている音楽データを携帯電話機100によって通常よりも安い料金で受信して聴くことができる。

【0195】さらに、本発明においては、配信サーバは、暗号化音楽データを携帯電話機100へ配信する際、位置情報に関連する画像データも一緒に配信しても良い。この画像データは、携帯電話機100の現在位置

が所在する地方の景色等である。携帯電話機100は、受信した画像データをディスプレイ1110に表示し、音楽を聴きながら、その地方の景色を楽しむことができる。

【0196】また、さらに、上記においては、配信サーバ30は携帯電話機100の現在位置を受信してから、その位置情報に関連する暗号化コンテンツデータの検索をするとして説明したが、配信サーバ30は、予め各位置情報に関連する暗号化コンテンツデータを分類して保持していても良い。

【0197】本発明の実施の形態によれば、携帯電話機は、現在位置に関連する暗号化コンテンツデータを受信し、音楽データを聴くことができるので、移動中に各地方に関連する音楽データを楽しむことができる。

【0198】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図1】 データ配信システムを概念的に説明する概略図である。

【図2】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図3】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図4】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図5】 ライセンスサーバの構成を示す概略ブロック図である。

【図6】 携帯電話機の構成を示すブロック図である。

【図7】 メモリカードの構成を示すブロック図である。

【図8】 図1に示すデータ配信システムにおける配信動作を説明するための第1のフローチャートである。

【図9】 図1に示すデータ配信システムにおける配信動作を説明するための第2のフローチャートである。

【図10】 図1に示すデータ配信システムにおける配信動作を説明するための第3のフローチャートである。

【図11】 図1に示すデータ配信システムにおける配

信動作を説明するための第4のフローチャートである。

【図12】 配信サーバから携帯電話機に送信されたメニューを携帯電話機の表示部に表示した状態を示す図である。

【図13】 携帯電話機における再生動作を説明するための第1のフローチャートである。

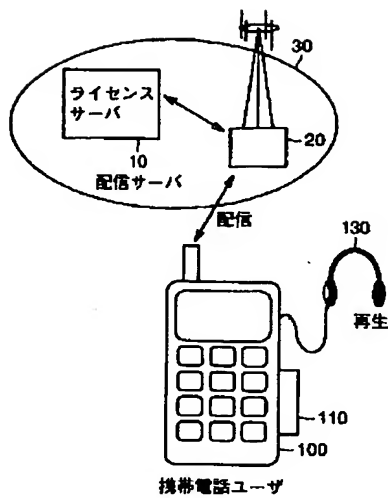
【図14】 携帯電話機における再生動作を説明するための第2のフローチャートである。

【図15】 携帯電話機の現在位置を検出するシステムを概念的に説明するための概略図である。

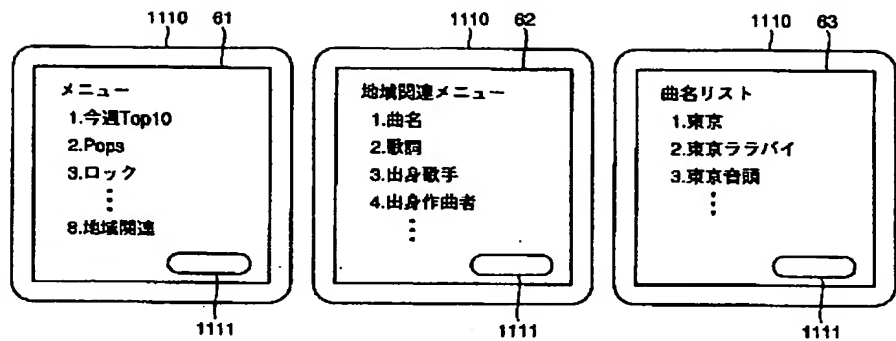
【符号の説明】

10 ライセンスサーバ、20 配信キャリア、30 配信サーバ、40 位置情報センター、41 地図データベース、42 基地局データベース、43 端末機位置データベース、50 電話網、51 公衆回線網、52 ~54 基地局、61 メニュー、62 ジャンルメニュー、63 項目メニュー、100 携帯電話機、110 メモリカード、130 ヘッドホン、1106, 1420 コントローラ、302 課金データベース、304 情報データベース、306 CRLデータベース、307 メニューデータベース、308 配信記録データベース、310 データ処理部、312, 320, 1206, 1212, 1214, 1404, 1408, 1412, 1422 復号処理部、313 認証鍵保持部、315 配信制御部、316, 1210, 1418 セッションキー発生部、318, 326, 328, 1208, 1406, 1410 暗号処理部、350 通信装置、1102 アンテナ、1104 送受信部、1108 キー操作部、1110 ディスプレイ、1111 移行部、1112 音声再生部、1113, 1218 DA変換器、1114, 1201, 1220, 1224 端子、1115 マイク、1116 AD変換器、1117 音声符号化部、1200 メモリインタフェース、1202, 1400 認証データ保持部、1204 Kp1保持部、1216 音楽再生部、1222 スイッチ、1402 Kmc1保持部、1414 KPma保持部、1415 メモリ、1415A CRL領域、1415B データ領域、1416 Kpm1保持部、1421 Km1保持部、1423 インタフェース、1440 ライセンス情報保持部、1442, 1444, 1446 切換スイッチ。

【図1】



【図12】



【図2】

名称	属性	保持/発生箇所	機能・特徴
Data	コンテンツデータ	配信サーバ	例：音楽データ、アップデートプログラム
Kc	ライセンス鍵		暗号化コンテンツデータの復号鍵
[Data]Kc	暗号化コンテンツデータ		共通鍵Kcで復号可能な暗号化が施されたコンテンツデータ この形式で配信サーバより配布。
Data-Inf	付加情報		例：コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報
コンテンツID	コンテンツに関する情報		コンテンツデータDataを識別するコード
ライセンスID	ライセンスに関する情報		ライセンスの発行を特定できる管理コード (コンテンツIDを含めて識別することも可)
トランザクションID	ライセンス固有		配信を特定するための管理コード
AC	ライセンス購入条件		利用者側から指定(例：ライセンス数、機能限定等)
AC1	アクセス制限情報		メモリのアクセスに対する制限(例：再生可能回数)
AC2	再生回路制御情報		コンテンツ再生回路(携帯電話機)における制御情報 (例：再生可否)

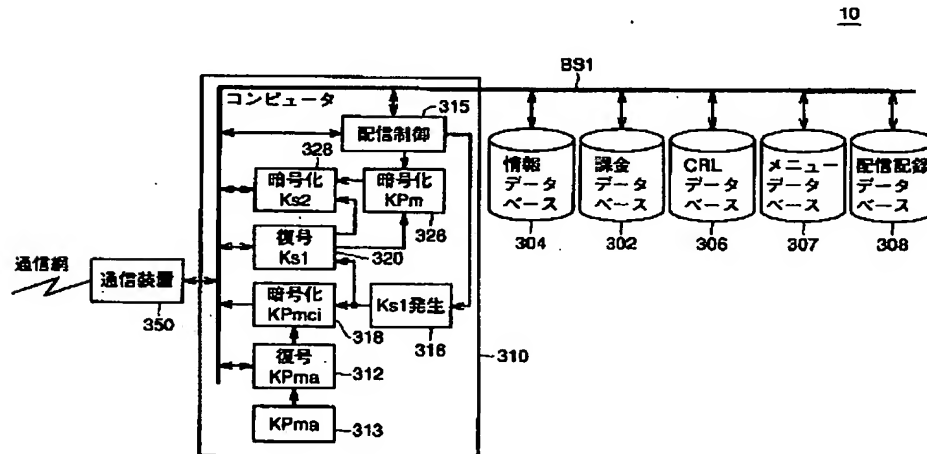
【図4】

名称	属性	保持/発生箇所	機能・特徴
Ks1	共通鍵	配信サーバ	配信セッション毎に発生
Ks2		メモリカード	配信/再生セッション毎に発生
Ks3		携帯電話機	再生セッション毎に発生
Km	秘密復号鍵	メモリカード	メモリカードごとに固有の復号鍵 KPmで暗号化されたデータはKmで復号可能
KPm	公開暗号鍵 (非対称鍵)	メモリカード	メモリカードごとに固有の暗号鍵
KPma	公開復号鍵	配信サーバ	配信システム全体で共通。

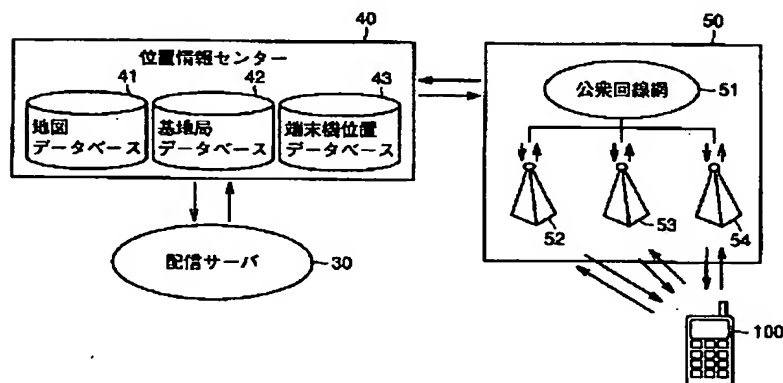
【図3】

名称	属性	保持/発生箇所	機能・特徴
CRL	禁止クラスリスト 関連情報	配信サーバ メモリカード	禁止クラスリストの対象クラスデータ
CRL_dat		配信サーバ	禁止クラスリストのバージョン更新のための情報
CRL_ver		メモリカード	禁止クラスリストのバージョン情報
KPpn	公開暗号鍵 (非対称鍵)	携帯電話機	KPpnにて復号可能。 (KPpn/Crtfn)KPmaの形式で出荷時に記録 *携帯電話機の種類nごとに異なる。
KPmci	公開暗号鍵 (非対称鍵)	メモリカード	Kmciにて復号可能。 (KPmci/Cmci)KPmaの形式で出荷時に記録 *メモリカードの種類nごとに異なる。
Kpn	秘密復号鍵	携帯電話機	コンテンツ再生回路(携帯電話機)固有の復号鍵 *携帯電話機の種類nごとに異なる。
Kmci	秘密復号鍵	メモリカード	メモリカード固有の復号鍵 *メモリカードの種類nごとに異なる。
Crtfn	クラス証明書	携帯電話機	コンテンツ再生回路のクラス証明書。認証機能を有する。 (KPpn/Crtfn)KPmaの形式で出荷時に記録 *携帯電話機のクラスnごとに異なる。
Cmci		メモリカード	メモリカードのクラス証明書。認証機能を有する。 (KPmci/Cmci)KPmaの形式で出荷時に記録 *メモリカードのクラスnごとに異なる。

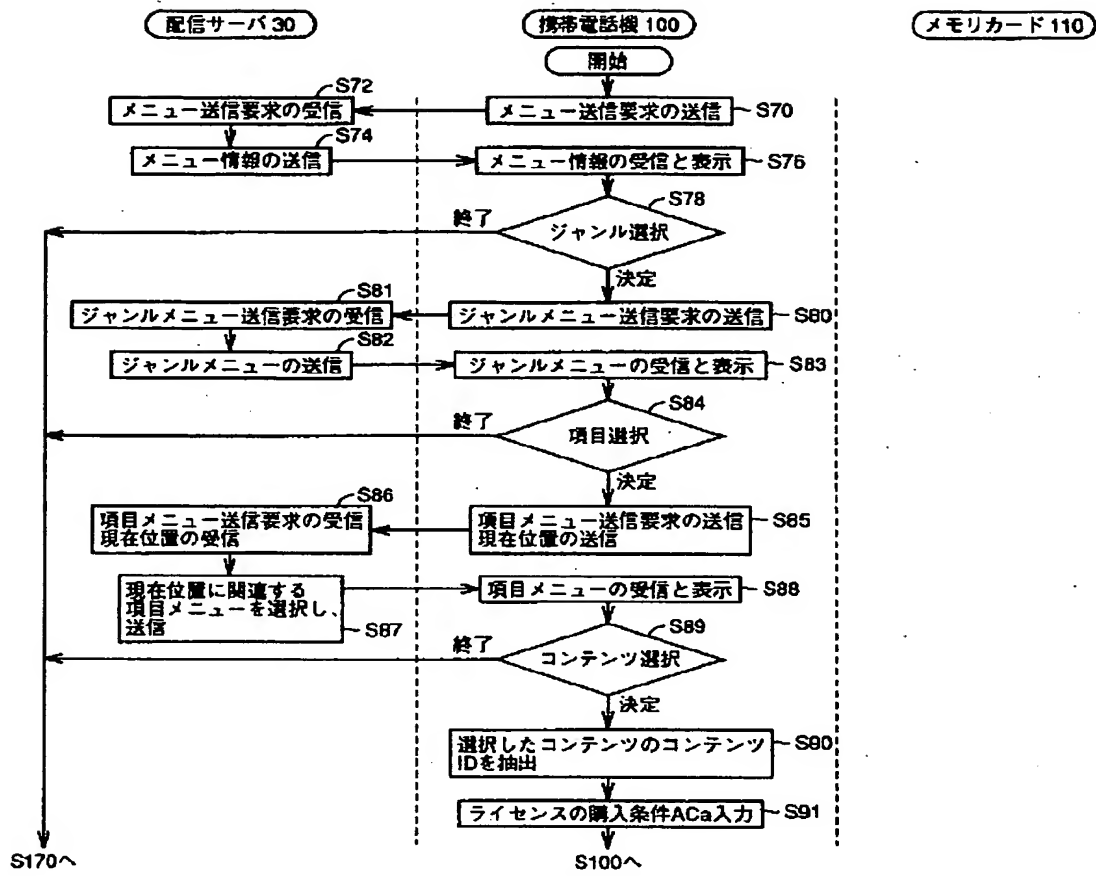
【図5】



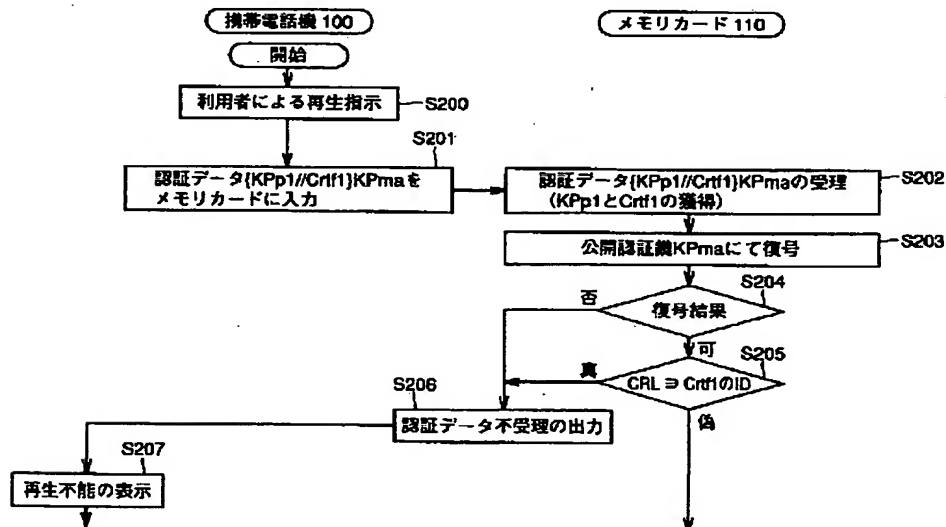
【図15】



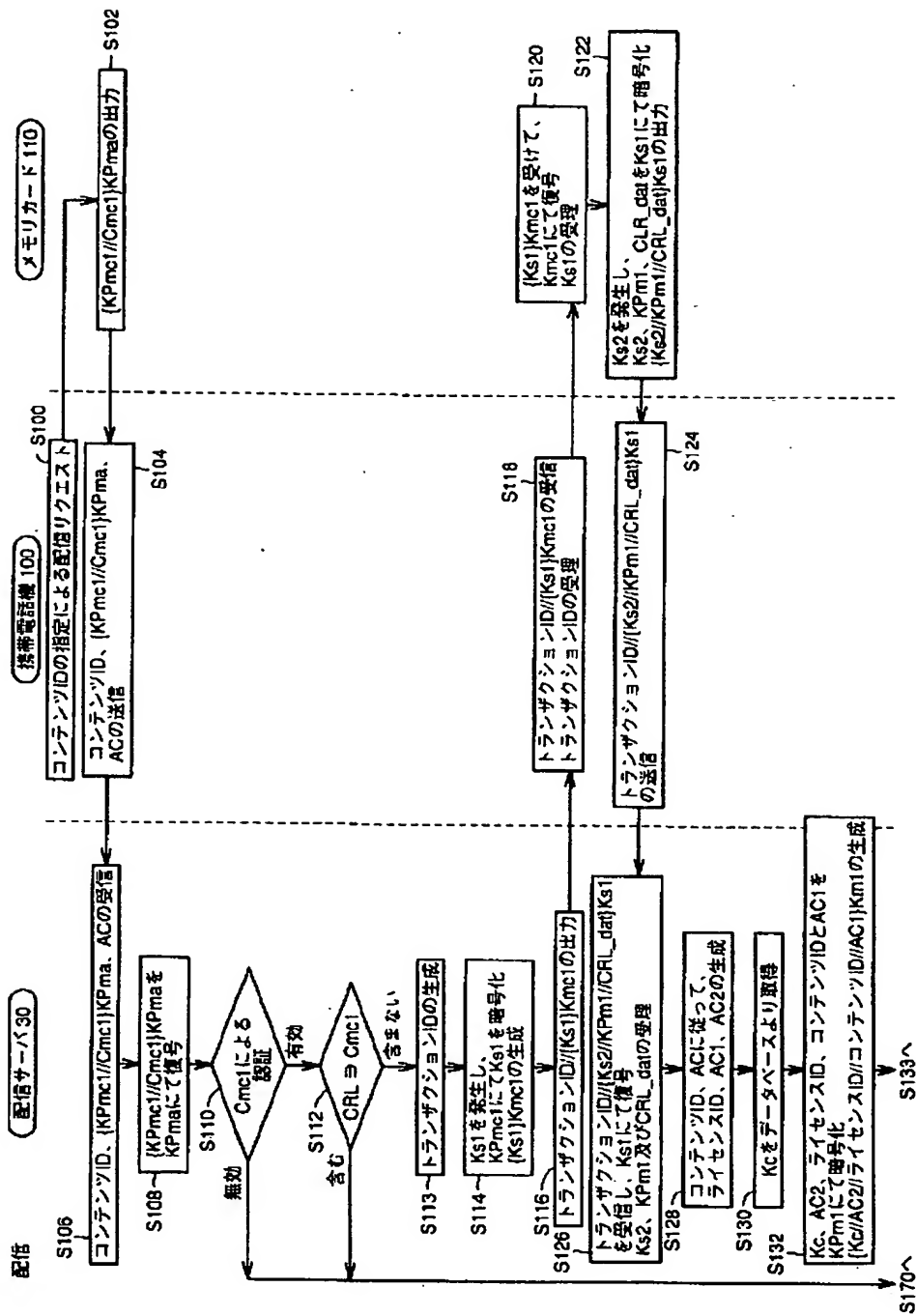
【図8】



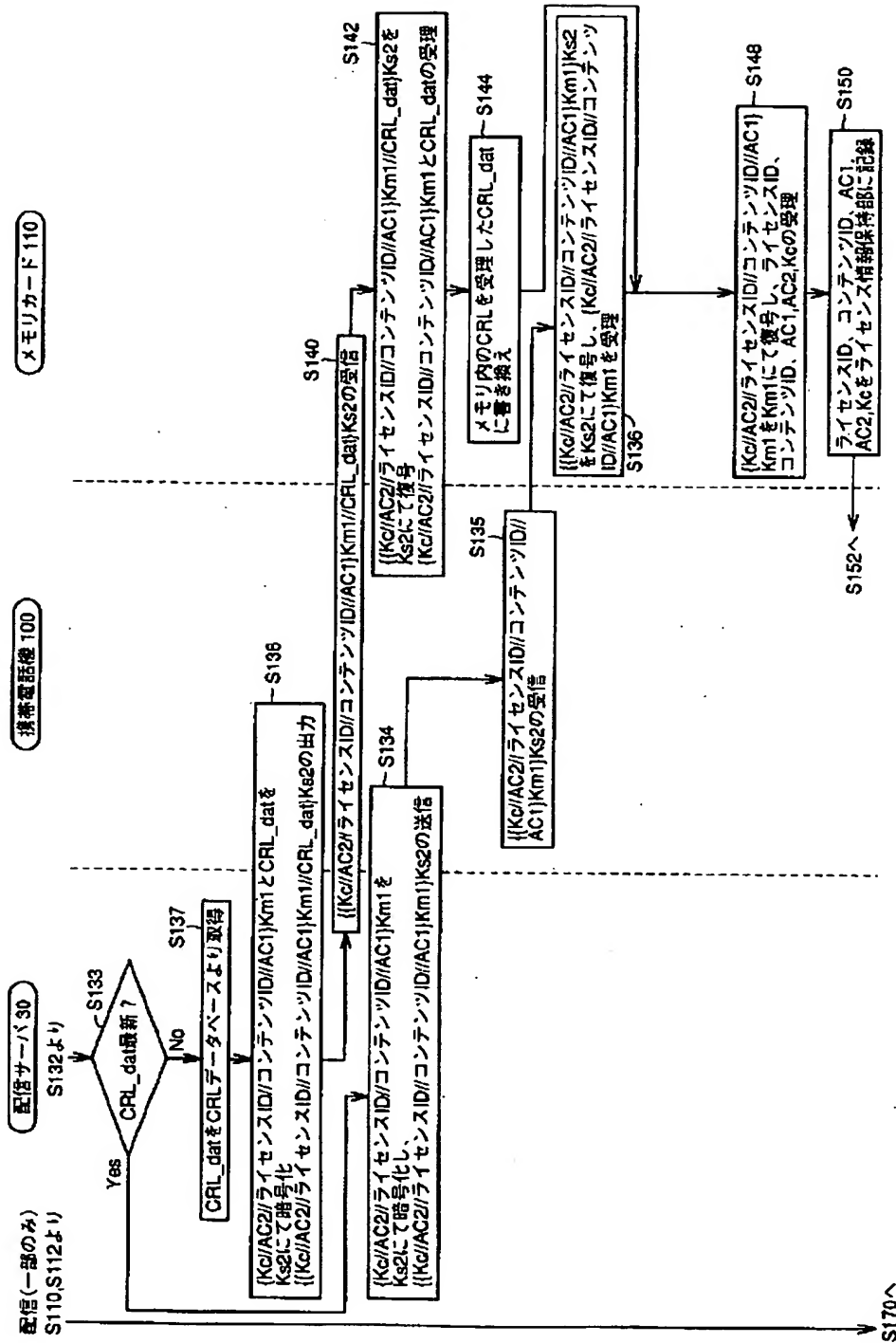
【図13】



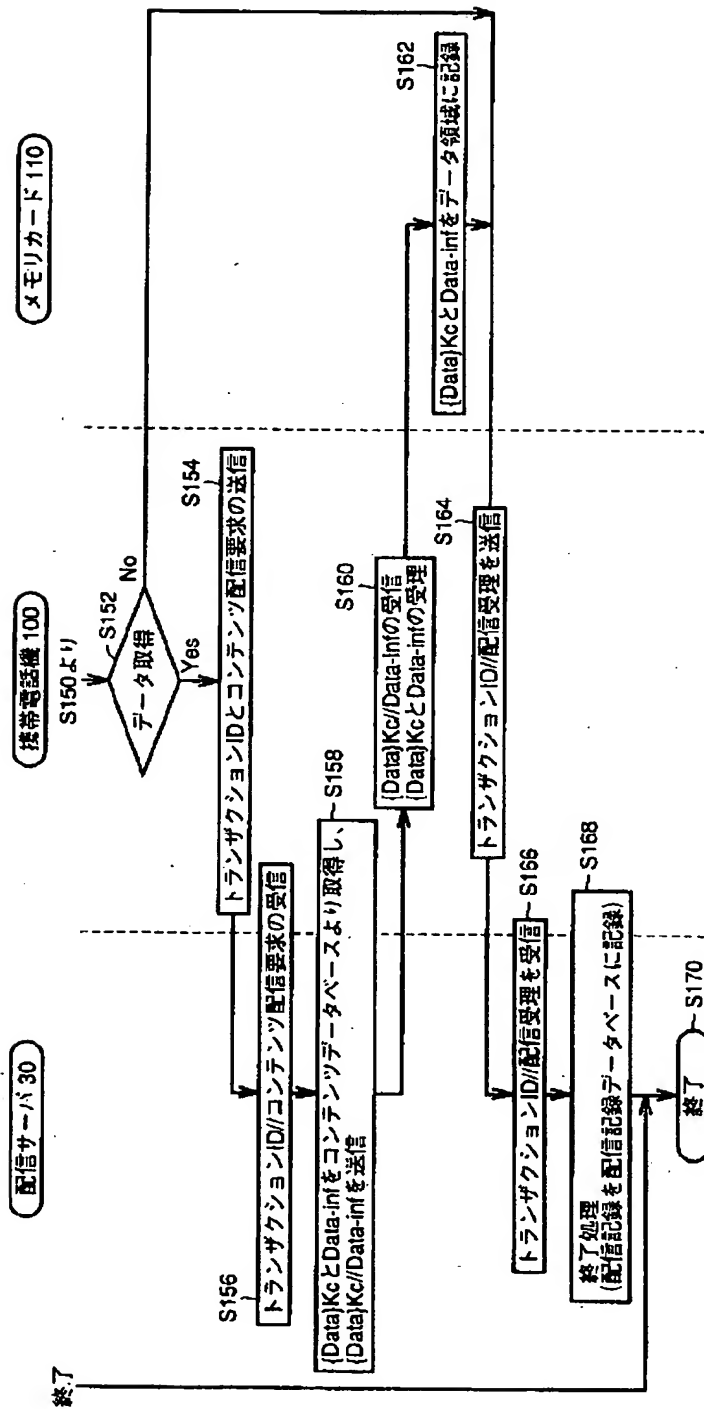
【図9】



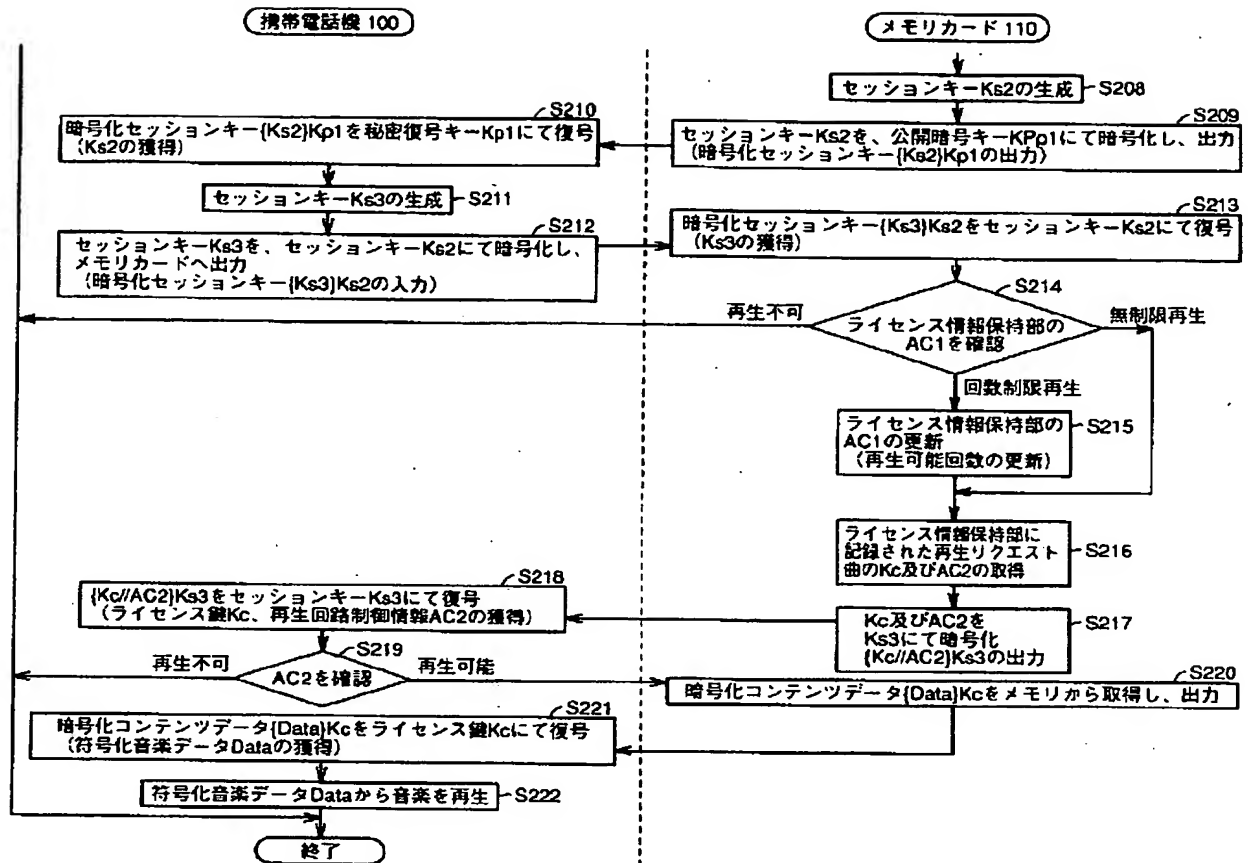
【図10】



【図11】



【図14】



フロントページの続き

(51)Int.Cl.'	識別記号	F I	テーマコード' (参考)
G 1 0 K 15/02		G 1 0 K 15/02	
G 1 0 L 19/00		H 0 4 M 1/00	R
H 0 4 M 1/00			3 0 2
	3 0 2	G 0 6 F 13/00	5 1 0 G
// G 0 6 F 13/00	5 1 0	G 1 0 L 9/00	N